

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSRComputer Law
&
Security Review

Ownership of personal data in the Internet of Things

Václav Janeček^{a,b,c,d,*}^a Oxford Internet Institute, University of Oxford, Oxford, United Kingdom^b Faculty of Law, University of Oxford, Oxford, United Kingdom^c St Edmund Hall, Oxford, United Kingdom^d Faculty of Law, Charles University, Prague, Czech Republic

ARTICLE INFO

Article history:

Available online xxx

Keywords:

Personal data

Personal information

Non-personal data

Data

Information

Ownership

Internet of Things

EU law

Property

GDPR

Review

ABSTRACT

This article analyses, defines, and refines the concepts of ownership and personal data to explore their compatibility in the context of EU law. It critically examines the traditional dividing line between personal and non-personal data and argues for a strict conceptual separation of personal data from personal information. The article also considers whether, and to what extent, the concept of ownership can be applied to personal data in the context of the Internet of Things (IoT). This consideration is framed around two main approaches shaping all ownership theories: a bottom-up and top-down approach. Via these dual lenses, the article reviews existing debates relating to four elements supporting introduction of ownership of personal data, namely the elements of control, protection, valuation, and allocation of personal data. It then explores the explanatory advantages and disadvantages of the two approaches in relation to each of these elements as well as to ownership of personal data in IoT at large. Lastly, this article outlines a revised approach to ownership of personal data in IoT that may serve as a blueprint for future work in this area and inform regulatory and policy debates.

© 2018 Dr Václav Janeček. Published by Elsevier Ltd. All rights reserved.

1. Introduction

Internet of Things (IoT) technologies are becoming increasingly more pervasive. Within the EU28 alone, the estimated number of connected ‘things’ was 1.8 billion in 2013 and is expected to reach 6 billion by 2020.¹ These so-called ‘smart’

devices will foster our interactions with the environment by facilitating transport and logistics, for example, as well as delivery of services like healthcare and security. At the same time, IoT devices generate and collect a wealth of personal data, whose management poses serious ethical² and

* Corresponding author at: St Edmund Hall, Queen’s Lane, OX1 4AR Oxford, United Kingdom.

E-mail address: vaclav.janecek@law.ox.ac.uk

¹ S Aguzzi and others, *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination* (European Commission 2014) 10, 26, 61. Globally, the number of connected devices is expected to grow from 9 billion in 2013 up to 50 billion by 2020: OECD, *OECD Digital Economy Outlook 2017* (OECD Publishing 2017) 247; GAO, *Technology assessment: Internet of Things: Status and implication of an increasingly connected world* (GAO-17-75, May 2017) 1;

McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* (McKinsey 2015) 17.

² J Van den Hoven, *Internet of Things Factsheet Ethics* (European Commission 2013).

<https://doi.org/10.1016/j.clsr.2018.04.007>

0267-3649/© 2018 Dr Václav Janeček. Published by Elsevier Ltd. All rights reserved.

legal³ questions. Ownership of personal data underpins the issues revolving around data management and control, such as privacy, trust,⁴ and security, and it has also important implications for the future of the 'digital' economy and trade in data.⁵ This is why debates on introducing the concept of data ownership as a legal right have recently emerged at the EU level⁶ and beyond,⁷ and why they are still thriving, although the majority of the legal doctrine and now also the European

Commission have reservations about the data ownership concept.

Due to legal developments in personal data protection, starting with the fundamental right to respect for private life,⁸ over the fundamental right to protection of personal data,⁹ and recently culminating by the data subject's rights granted by the General Data Protection Regulation (GDPR),¹⁰ it became impossible to think of any data ownership without also thinking about ownership of *personal* data. The problem is, however, that the line between personal and non-personal data is a moving target and data that are now seen as non-personal data may become (thanks to analytical and technological advancements) personal data in the future.¹¹ Thus, exploring the conceptual limits of ownership of personal data must precede debates on ownership of purely non-personal data (e.g. data employed in smart farming).¹² In fact, personal data have already been recognized as one of the key economic assets,¹³ and avoiding questions regarding their ownership is thus problematic even in the light of these economic trends. Moreover, the need for the analysis stems from the nature of the IoT world in which many of us already live. Take, for instance, 'smart cities' where big data companies may soon be able to privatize data (including personal data), despite them being largely collected without prior consent of data subjects.¹⁴ In response to these challenges, a number of ownership-like types of technological solution are also emerging. One such example is the AURA platform—a Personal In-

³ See J Drexel and others, 'Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate' (2016) *Max Planck Institute for Innovation & Competition Research Paper No 16-10* <<https://ssrn.com/abstract=2833165>> accessed 16 November 2017.

⁴ M Taddeo, 'Trusting Digital Technologies Correctly' (2017) 27 *Minds & Machines* 565; M Taddeo, 'Trust in Technology: A Distinctive and a Problematic Relation' (2010) 23 *Know Tech Pol* 283.

⁵ See, e.g., TJ Farkas, 'Data Created by the Internet of Things: The New Gold without Ownership' (2017) 23 *Rev Prop Intmaterial* 5, 14; C Bartolini, C Santos and C Ullrich, 'Property and the cloud' (2018) 34 *CLSR* 358; V Gazis and others, 'Short Paper: IoT: Challenges, projects, architectures' (2015) 18 *International Conference on Intelligence in Next Generation Networks* 145; A Whitmore, A Agarwal and L Da Xu, 'The Internet of Things—A survey of topics and trends' (2015) 17 *Inf Syst Front* 261, 266; IERC – European Research Cluster on the Internet of Things, *Internet of Things: IoT governance, privacy and security issues* (European Commission 2015) 10, 78–79.

⁶ See, e.g., Commission, 'Building a European Data Economy' (Communication) COM (2017) 9 final, 9–10, 13; Commission, 'On the free flow of data and emerging issues of the European data economy, accompanying COM (2017) 9 final' (Commission Staff Working Document) SWD (2017) 2 final, esp. 23, 33–38; Osborne Clarke LLP, *Legal study on ownership and access to data* (European Commission 2016) <<https://bookshop.europa.eu/en/legal-study-on-ownership-and-access-to-data-pbKK0416811/>> [<https://perma.cc/82D8-9787>]; N Duch-Brown, B Martens and F Mueller-Langer, 'The Economics of Ownership, Access and Trade in Digital Data' (JRC Digital Economy Working Paper 2017-01, European Commission 2017) 12ff <<https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf>> [<https://perma.cc/NUM8-HVWB>]; A Gärtner and K Brimsted, 'Let's talk about data ownership' (2017) 39 *EIPR* 461; S van Erp, 'Ownership of Data: The Numerus Clausus of Legal Objects' (2017) 6 *Brigham-Kanner Property Rights Conference Journal* 235; S Lohsse, R Schulze and D Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos/Hart Publishing 2017); F Thouvenin, RH Weber and A Früh, 'Data ownership: Taking stock and mapping the issues' in M Dehmer and F Emmert-Streib (eds), *Frontiers in Data Science* (CRC Press 2018). Thanks is due to Stephen Saxby for bringing my attention to the 2018 publication.

⁷ Globally, see, e.g., IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (version 2) (IEEE 2017) 141–42, 237–38, 247 [<https://perma.cc/W5MT-VK9K>]; McKinsey Global Institute (n 1) 11, 26, 104, 106, 107 and 113. For India, see Telecom Regulatory Authority of India, *Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector* (TRAI Consultation No 09/2017) 2 and 6 [<https://perma.cc/ES29-ZVA4>]. Thanks is due to Ashok Rajagopalan for bringing my attention to this Indian document. For Australia, see Productivity Commission, *Data Availability and Use* (Report No 82, 2017) 53, 65, 66, 177, 191, 196, 241 and 584 [<https://perma.cc/6RKE-PCGL>]. For China, see Arts 45 and 48 of the First Draft E-Commerce Law of the People's Republic of China (published 27 December 2016). Thanks is due to Vicky Cheng for bringing my attention to this Chinese document. For the USA, see

Osborne Clarke LLP (n 6) 78–81. For the United Kingdom (if seen as a potential non-EU member), see <<http://www.parliament.uk/business/lords/media-centre/house-of-lords-media-notice/house-of-lords-media-notice-2017/october-2017/who-should-own-your-data/>> [<https://perma.cc/73JB-8QJU>].

⁸ Art 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms 1950.

⁹ Art 8 of the Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

¹⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/2016).

¹¹ C Wendehorst, 'Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy' in Lohsse, Schulze and Staudenmayer (eds) (n 6) 332.

¹² See S Wolfert and others, 'Big Data in Smart Farming – A review' (2017) 153 *Agricultural Systems* 69; J Drexel, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) 8 *JIPITEC* 257. cf also Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union' COM (2017) 495 final; Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM (2017) 10 final.

¹³ World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (Geneva 2011) <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf> [<https://perma.cc/T7JL-BZXX>].

¹⁴ See I Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2 *EDPLR* 28, 33–34.

Download English Version:

<https://daneshyari.com/en/article/10225858>

Download Persian Version:

<https://daneshyari.com/article/10225858>

[Daneshyari.com](https://daneshyari.com)